14.3 Cryptographie asymétrique

NSI terminale - JB Duthoit

14.3.1 Un exemple avec *Le puzzle de Merkel*

Exercice 14.10

1. Question préliminaire :
   On considère le message codé :

   ```
   secret = '*( (7%#/""1|c|wwsxp~tu}jc/)¯ylqs{y|s%vil&ys~'
   ```

   Décrypter ce message en sachant qu'il a été créé avec une clé "courte" et que le début du message est "identifiant".

2. On imagine dans la suite que Alice veut envoyer un message à Bob, sans que Eve puisse intercepter le message !
   Le puzzle de Merkel fonctionne selon le principe suivant :

   a) Alice va créer un fichier de 1 000 000 de lignes, chaque ligne étant un message du type de la question préliminaire, avec un clé de chiffrement différente et "courte' pour chaque ligne.

   b) Alice envoie ce fichier à Bob. Ève est donc en mesure de l'intercepter.

   c) Bob reçoit le fichier, choisit une ligne au hasard et décrypte le message à l'aide d'un algorithme de force brute (ceci est possible car la clef de chiffrement est courte).
   Il obtient donc un fichier du type :
   identifiant : 8785452132, clé : sledj#45P9878al

   d) Bob envoie à Alice, en clair, le numéro d'identifiant (et lui seul) . Eve peut intercepter ce message, mais que peut-elle en faire ?

   e) Alice possède bien évidemment le fichier de 1 000 000 de lignes non chiffrées. C'est donc très facile pour elle de connaître la ligne choisie par Bob !

   f) Alice et Bob ont maintenant une clef longue afin de coder leurs futurs échanges (la clef noté après les identifiants).

   ☛ Bien sûr, Eve peut tenter de déchiffrer les lignes, mais cela prendra du temps. On peut considérer que si le déchiffrement d'une ligne prend 1 seconde, il faudra en moyenne 500 000 secondes pour déchiffrer les 1 000 000 de lignes, soit plus de 5 jours !

⚠ La méthode des puzzle de Merkle, bien que novatrice pour son époque, n'est plus jugée suffisante de nos jours pour garantir une véritable sécurité.

14.3.2 Principe du chiffrement asymétrique

Savoir-Faire 14.3 : Décrire le fonctionnement du chiffrement asymétrique (clé privé / clé publique)

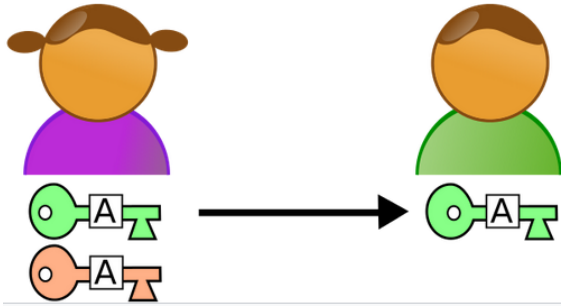
- Vous devez être capable de décrire le fonctionnement du chiffrement asymétrique.
- Connaître les avantages et inconvénients du chiffrement asymétrique.

Analogie : la boîte à deux serrures

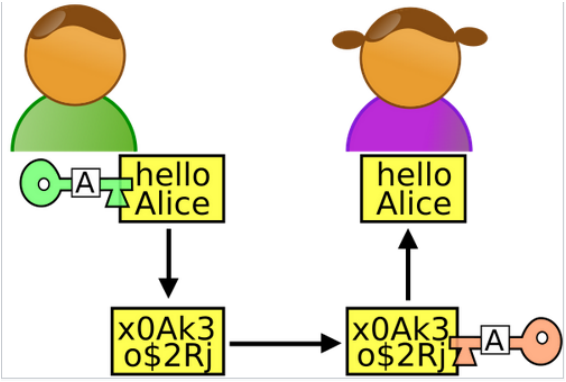
Une analogie envisageable serait d'imaginer une boîte avec deux serrures différentes. Lorsque l'on ferme la boîte d'un côté, seule la clef correspondant à l'autre serrure permet l'ouverture de la boîte et vice-versa
Une des clefs est privée et conservée secrète, l'autre est dite publique et un exemplaire peut-être obtenu par quiconque souhaite utiliser la boîte.

Pour chiffrer un message Bob prend la boîte, y place son message, et la ferme à l'aide de la clef publique. Seul le détenteur de la clef privée permettant d'accéder à l'autre serrure, Alice en l'occurrence, sera en mesure de rouvrir la boîte.

Principe du chiffrement asymétrique



1re étape : Alice génère deux clefs. La clef publique (verte) qu'elle envoie à Bob et la clef privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.

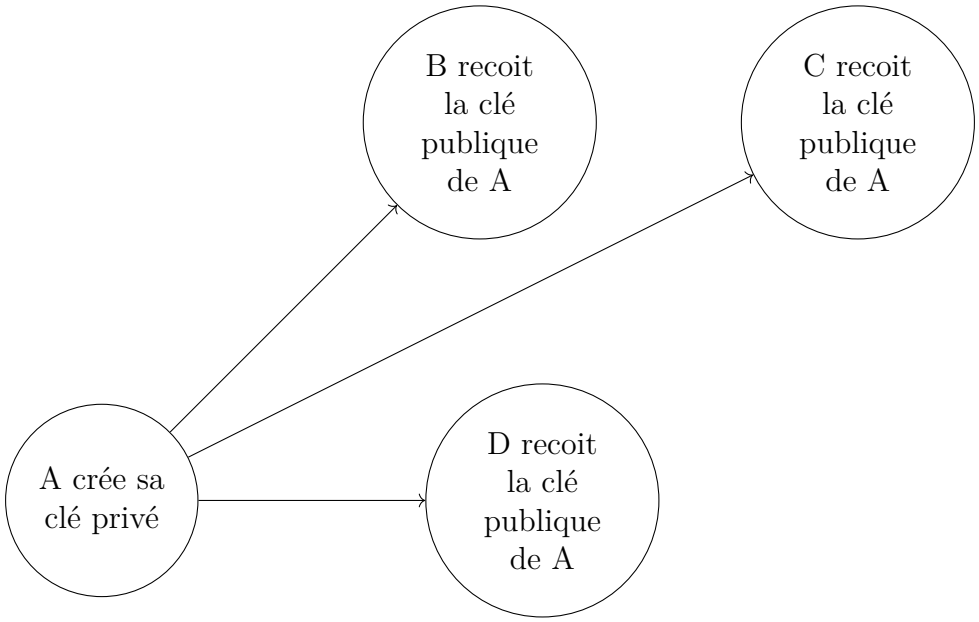


2e et 3e étapes : Bob chiffre le message avec la clef publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clef privée.

Supposons que (A) ait l'envie d'envoyer un message à (B), (C) et (D) de façon sécurisée. (A) doit créer une clé de chiffrement privé (clé privé) et le garde pour lui précieusement. A partir de sa clé privée, il crée une clé publique qu'il diffuse largement.

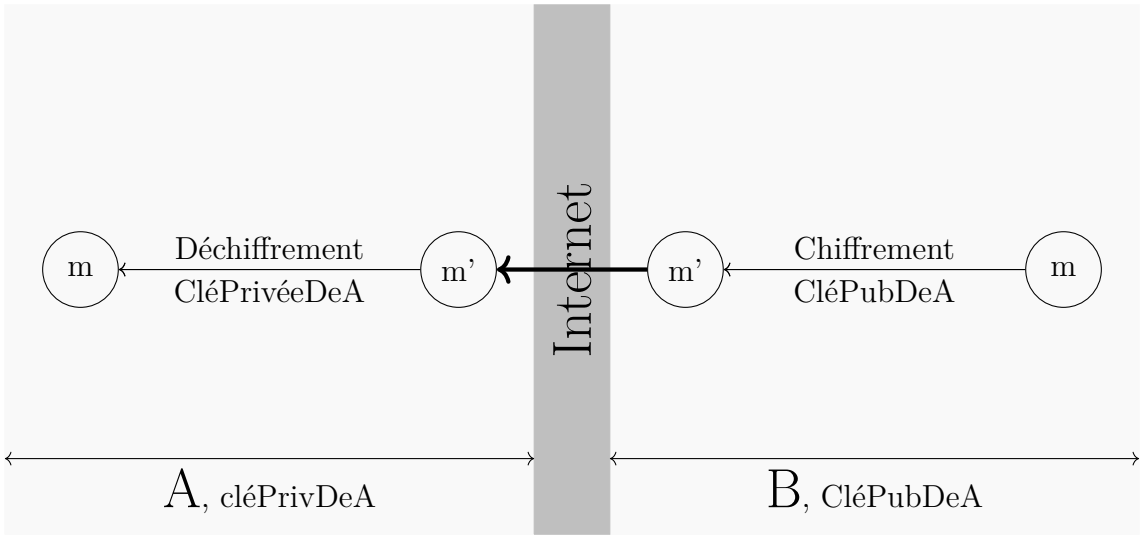
⚠ Bien évidemment, le système repose sur le fait qu'il est impossible de trouver la clé privé à partir de la clé publique.

Génération des clés

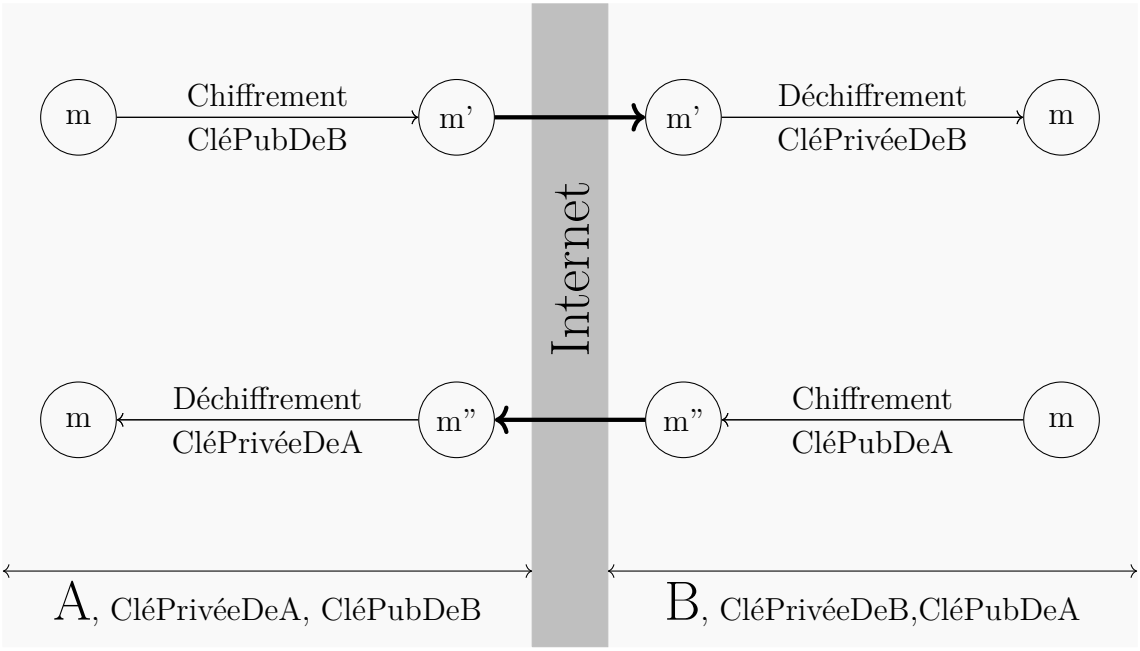


⚠ La clé publique va servir à chiffrer lors de l'envoi et la clé privée à déchiffrer lors de la réception :

Envoi d'un message de (B) vers (A)



Envoi et réception de message



14.3.3 Un exemple : le RSA

Prenons un exemple : l'algorithme de chiffrement asymétrique RSA est très couramment utilisé, notamment dans tout ce qui touche au commerce électronique.
RSA se base sur la factorisation des très grands nombres premiers. Si vous prenez un nombre premier A (par exemple A = 16813007) et un nombre premier B (par exemple B = 258027589), il facile de déterminer C le produit de A par B (ici on a A x B = C avec C = 4338219660050123). En revanche si je vous donne C (ici 4338219660050123) il est très difficile de retrouver A et B. En tous les cas, à ce jour, aucun algorithme n'est capable de retrouver A et B connaissant C dans un temps "raisonnable". Nous avons donc bien ici un problème relativement facile dans un sens (trouver C à partir de A et B) est extrêmement difficile dans l'autre sens (trouver A et B à partir de C).

14.3.4 Méthode de Diffie-Hellman

Cette méthode repose sur l'utilisation d'une fonction mathématique à deux variables. Cette fonction, souvent nommée M
(pour "Mélange"), doit respecter les propriétés suivantes :

1. M est connue, ce qui signifie qu'on connait l'algorithme ou la formule qui permet de calculer des images (toutes les fonctions ne sont pas calculables, voir théorie de la calculabilité).

2. Si on connait $M(x; y)$ et x, il doit être très difficile de retrouver y. Par difficile, on entend le fait que pour trouver le y donnant à $M(x; y)$ une valeur donnée, il faudra essayer sur tous les entiers y possibles.

3. Pour tous entiers x, y et z, on a $M(M(x; y); z) = M(M(x; z); y)$. Autrement y et z sont commutables.

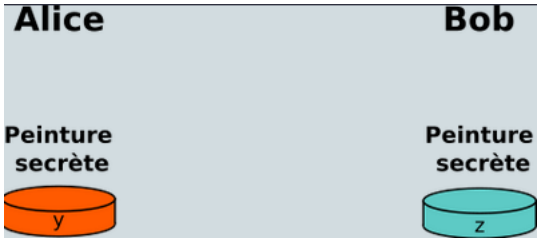
Une analogie couramment utilisée pour expliquer le fonctionnement de cette fonction est celle des pots de peinture :

1.

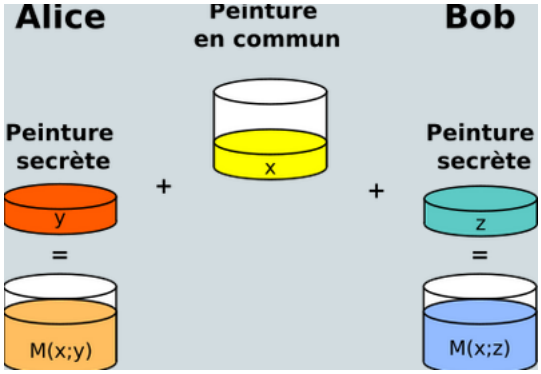
On dispose d'un très grand nombre de pots de peinture de couleurs différentes. Alice et Bob se mettent d'accord pour choisir une couleur commune x , qui sera "publique", puisqu'elle peut être interceptée.



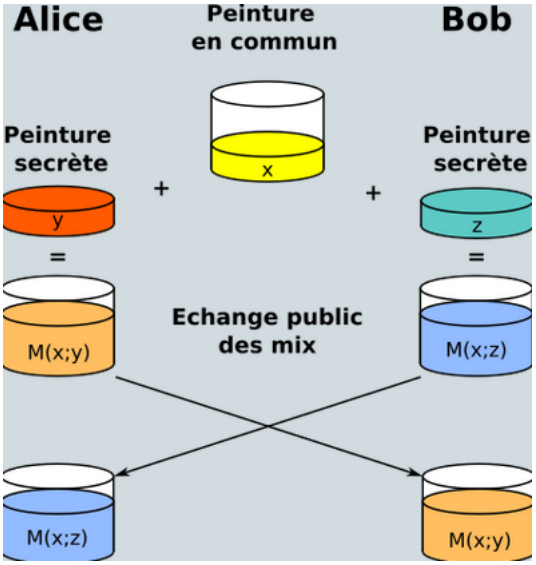
2. Alice et Bob choisissent alors chacun une couleur, respectivement y et z, qui resteront privées et secrètes et ne seront jamais échangées.



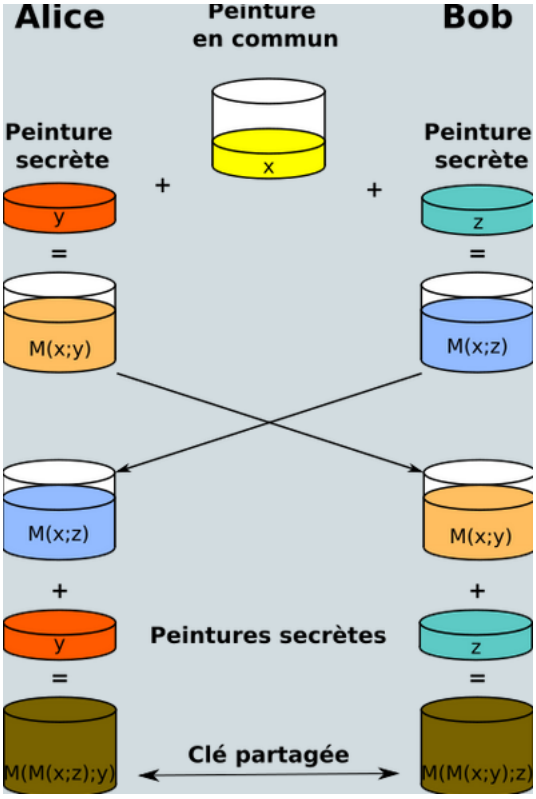
3. Alice et Bob élaborent alors leurs mélanges, en utilisant la couleur commune et leur propre couleur privée.



4. Alice et Bob échangent en clair leurs mélanges respectifs, qui peuvent donc être interceptés.

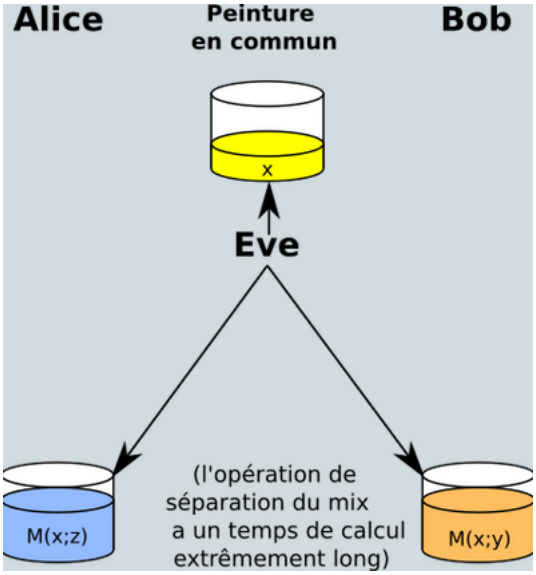


5. Alice et Bob ajoutent alors au mélange qu'ils ont reçu leur couleur secrète. La fonction de mélange est construite afin que les mix obtenus par Alice et Bob soient identiques. Ils ont ainsi une "couleur" commune secrète, qui peut alors leur permettre d'effectuer des échanges via un cryptage symétrique.



6. Ève peut connaitre trois choses : la couleur commune, et chacun des mix ayant circulé en clair. Pour autant, la fonction de mélange est faite de telle manière qu'il soit extrêmement long et difficile d'extraire les couleurs secrètes même si la couleur commune est connue.

   Par ailleurs, même en mélangeant les deux mix obtenus, on n'obtiendra pas la même couleur que celle obtenue par Alice et Bob, puisque la couleur commune sera deux fois plus présente.



Le protocole d'échange de clé de Diffie-Hellman propose donc une manière élégante de régler le problème d'échange de clé posé par le chiffrement symétrique. Cependant, un problème reste à régler, il s'agit du problème de l'authentification : la sureté des communications dépend essentiellement sur le fait qu'Alice et Bob soient certains de communiquer avec la bonne personne.